Claims

1. Method for protecting at least one motor vehicle component against manipulation in a control device, which comprises at least one microcomputer (μC) and at least one memory module (2, 3), characterized in that the code necessary for operation of the control device (1) is divided into at least one master code (MC) which comprises information essential for operation of the control device (1), and at least one sub-code (SC) which comprises additional information for operation of the control device (1), at least the master code (1) being stored in the microcomputer (μC) and the master code (MC) monitoring the manipulation of the sub-code (SC).

2. The process as claimed in claim 1, wherein the master code (MC) is stored in a read-protected area (11) of the microcomputer (μC) which is writable only once.

3. The process as claimed in one of claims 1 or 2, wherein the sub-code (SC) is stored in a rewritable area of the microcomputer.

4. The process as claimed in one of claims 1 or 2, wherein the sub-code (SC) is stored in a rewritable area of at least one external memory module (2).

5. Control device for a motor vehicle component which comprises at least one microcomputer (μC) and at least one memory module (2, 3), the code which is necessary for operation of the control device (1) being divided into at least one master code (MC) which comprises information which is essential for operation of the control device (1), and at least one sub-code (SC) which comprises additional information for operation of the control device (1), and at least the master code (MC) being stored in the microcomputer (μC) and the master code (MC) containing a software function module for detection of manipulation within the sub-code (SC).

6. The control device as claimed in claim 5, wherein the master code (MC) is stored in a read-protected area (11) of the microcomputer (μC) which is writable only once.

7. The control device as claimed in claim 5 or 6, wherein the sub-code (SC) is stored in a rewritable area of the microcomputer (μC).

8. The control device as claimed in claim 5 or 6, wherein the sub-code (SC) is stored in a rewritable area of at least one external memory module (2, 3).

9. The control device as claimed in one of claims 5 to 8, wherein at least one part of the sub-code (SC) is stored encrypted in a rewritable area and the master code (MC) is used to generate a key for decryption.